



**Homeland
Security**

Daily Open Source Infrastructure Report

04 November 2015

Top Stories

- The U.S. Department of Justice reported November 2 that Netcracker Technology Corp., agreed to pay \$11.4 million and Computer Sciences Corp., agreed to pay \$1.35 million for allegedly using individuals on a Defense Information Systems Agency contract without proper security clearances. – *U.S. Department of Justice* (See item [1](#))
- The Fairfax County superintendent announced November 2 the suspension of all science experiments involving open flames until further notice after an October 30 incident at W.T. Woodson High School injured 5 students and a teacher. – *Washington Post* (See item [12](#))
- The U.S. Department of Justice will release 6,000 inmates from Federal prisons between October 30 and November 2 as part of its plan to reduce prison crowding and long punishments given to drug offenders. – *WBIR 10 Knoxville* (See item [15](#))
- Trend Micro researchers reported the Moplus software development kit offered by Baidu includes a functionality that can be abused to install backdoors on users' devices via a Hypertext Transfer Protocol server on the targeted smartphone. – *Softpedia* (See item [16](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)

Energy Sector

Nothing to report

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

1. *November 2, U.S. Department of Justice* – (National) Netcracker Technology Corp. and Computer Sciences Corp. agree to settle Civil False Claims Act allegations. The U.S. Department of Justice announced November 2 that Netcracker Technology Corp., agreed to pay \$11.4 million and Computer Sciences Corp., agreed to pay \$1.35 million to settle charges that the companies allegedly used individuals on a Defense Information Systems Agency (DISA) contract without proper security clearances, violating the False Claims Act from 2008 through 2013.
Source: <http://www.justice.gov/opa/pr/netcracker-technology-corp-and-computer-sciences-corp-agree-settle-civil-false-claims-act>

Financial Services Sector

2. *November 2, Reuters* – (California) JPMorgan settles California debt collection charges. JPMorgan Chase & Co., agreed to pay \$50 million in a settlement with the State of California to resolve allegations that the company tried to collect incorrect sums, sold bad credit card debt, engaged in “robosigning” of thousands of court documents never reviewed, and improperly obtained default judgements against military personnel November 2 after withholding from a July JPMorgan’s \$216 million settlement for related charged by the Federal government.
Source: <http://www.reuters.com/article/2015/11/02/us-jpmorgan-california-settlement-idUSKCN0SR2AU20151102>

Transportation Systems Sector

3. *November 2, KTTC 10 Rochester* – (Minnesota) Sheriff says two anhydrous ammonia leaks near Elkton “too much of a coincidence.” A 4-mile area of Interstate 90 in Elkton-Dexter area was shut down for 4 hours November 2 due to elevated levels of anhydrous ammonia in the air following 2 separate tank leaks. Fire officials and HAZMAT crews cleared the scene once the gas dissipated.

Source: <http://www.kttc.com/story/30414986/2015/11/02/update-i-90-reopens-after-being-closed-because-of-two-anhydrous-ammonia-leak-in-area>

4. *November 2, KTVU 2 Oakland* – (California) **2 separate crashes cause major delays on Hwy 580.** Interstate 580 near Livermore was shut down for several hours November 2 following two separate accidents in which an overturned semi-truck spilled its haul of frozen chicken and another accident in which a semi-truck collided with an SUV. Crews worked to clear the scenes and no injuries were reported.
Source: <http://www.ktvu.com/news/43317445-story>

5. *November 2, Associated Press* – (California) **Dust storm triggers 20-vehicle crash on highway in Bakersfield.** State Route 99 in southern San Joaquin Valley was shut down for several hours November 2 due to a 20-vehicle crash, caused by rain and snow. Five people were taken to area hospitals for minor injuries and the incident caused power outages in surrounding areas.

Source: <http://www.nbclosangeles.com/news/local/20-Vehicle-Crash-in-Bakersfield--339630082.html>

Food and Agriculture Sector

6. *November 2, U.S. Food and Drug Administration* – (Florida; Georgia; South Carolina) **Harveys and Winn-Dixie recall various Bakery Oatmeal Raisin Cookie products.** Jacksonville, Florida-based Southeastern Grocers issued a recall October 29 for 12-count, 18-count, and 20-count Bakery Oatmeal Raisin Cookies and Bakery Variety Pack Cookies, as well as its 36-count and 48-count Bakery Cookie Platters products due to misbranding and undeclared walnuts. The products were sold at certain Harveys and Winn-Dixie stores in Florida, Georgia, and South Carolina.
Source: <http://www.fda.gov/Safety/Recalls/ucm470517.htm>

7. *November 2, U.S. Department of Labor* – (Wisconsin) **Workers at IPMF LLC exposed to dangerous machine parts.** The Occupational Safety and Health Administration cited Beloit, Wisconsin-based IPMF LLC, operating as IPM Foods, October 30 for 1 willful, 12 serious, and 1 other-than-serious safety violations following a May 2015 complaint investigation that revealed the company did not use locking devices to prevent unintentional operation during service and maintenance and allowed employees to work on live electrical circuits, among other hazards. Proposed penalties total \$103,600.

Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=28980

8. *October 30, U.S. Department of Agriculture* – (New Jersey) **Joseph Epstein Food Enterprises, Inc. recalls Gluten-Free Turkey Meatball products due to misbranding.** East Rutherford, New Jersey-based Joseph Epstein Food Enterprises, Inc., issued a recall for approximately 190 pounds of its Mama Mancini's Slow Cooked Italian Style Sauce and Turkey Meatballs – Gluten Free products October 30 due to misbranding after a third party laboratory testing revealed the products contained an

excess amount of gluten for a product labeled as “gluten-free.” The items were sold at retail locations in New Jersey.

Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-134-2015-release>

Water and Wastewater Systems Sector

9. *November 2, Temple Daily Telegram* – (Texas) **Temple cleaning up 790,000 gallons of overflowed wastewater.** Temple city crews worked to clean up and disinfect 790,000 gallons of wastewater overflow November 2 after recent heavy storms flooded four wastewater systems. City officials reported the overflow did not affect the city’s drinking water supply.

Source: http://www.tdtnews.com/news/article_e0edd64c-81a0-11e5-bba9-b30e78c52cbf.html

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

10. *November 3, Associated Press* – (Illinois) **Chicago elementary school reopens after carbon monoxide leak.** Classes resumed November 2 at Prussing Elementary School in Chicago after new carbon monoxide detectors were installed in the building following an October 30 incident where 71 students and 7 staff members were hospitalized due to a carbon monoxide leak caused by a boiler.

Source: <http://www.fox32chicago.com/news/local/43769605-story>

11. *November 2, Dothan Eagle* – (Alabama) **Headland schools closed until Thursday due to storm damage.** Headland High School and Headland Elementary School in Henry County were closed November 2 due to storm damage overnight. School officials decided that the school buildings will remain closed through at least November 5 while crews work to repair damage, and classes will continue in portable classrooms on campus.

Source: http://www.dothaneagle.com/news/education/headland-schools-closed-until-thursday-due-to-storm-damage/article_c87e7d72-8188-11e5-ac34-0f8411207a2e.html

12. *November 2, Washington Post* – (Virginia) **School system bans open-flame science experiments after accident.** The Fairfax County superintendent announced November 2 the suspension of all science experiments involving open flames until further notice following an October 30 incident at W.T. Woodson High School where a teacher used a flammable liquid during a science demonstration, prompting a fire that hospitalized 5 students, injured the teacher, and evacuated the school.

Source: https://www.washingtonpost.com/local/education/school-system-bans-open-flame-science-experiments-after-accident/2015/11/02/ac5aad7a-8163-11e5-8ba6-cec48b74b2a7_story.html

13. *November 2, WMAQ 5 Chicago* – (Illinois) **27 transported to hospitals after school bus accident in Chicago.** An accident on Chicago's Northwest Side involving a school bus caused 27 people to be transported to area hospitals with injuries November 2. The cause of the accident is under investigation.
Source: <http://www.nbcchicago.com/traffic/transit/Bus-Accident-Reported-on-Chicagos-Northwest-Side-339554542.html>

For another story, see item 1

Emergency Services Sector

14. *November 3, WEWS 5 Cleveland* – (Ohio) **2 guards injured, 13 juveniles facing charges after riot at Canton detention center.** A November 2 riot at the Multi-County Juvenile Attention System in Canton left two guards injured when a fight broke out between juvenile detainees in a holding area. Thirteen juveniles are facing charges following the riot.
Source: <http://www.newsnet5.com/news/local-news/oh-stark/2-guards-injured-13-juveniles-facing-charges-after-riot-at-canton-detention-center>
15. *November 2, WBIR 10 Knoxville* – (National) **Inmates set free in largest one-time release from federal prison.** The U.S. Department of Justice will release 6,000 inmates from Federal prisons between October 30 and November 2 as part of its plan to reduce prison crowding and long punishments given to drug offenders.
Source: <http://www.wbir.com/story/news/local/2015/11/02/inmates-set-free-in-largest-one-time-release-from-federal-prison/75061044/>

Information Technology Sector

16. *November 3, Softpedia* – (International) **100 million Android users may have a backdoor on their device thanks to the Baidu SDK.** Researchers from Trend Micro reported the Moplus software development kit (SDK) being offered by Chinese search engine, Baidu includes a functionality that can be abused to install backdoors on users' devices via an Hypertext Transfer Protocol (HTTP) server on the targeted smartphone, allowing attackers to send HTTP requests to port 6259 or 40310 and execute malicious commands. The vulnerability has been included on an estimated 14,112 Android applications, potentially impacting over 100 million Android users.
Source: <http://news.softpedia.com/news/100-million-android-users-may-have-a-backdoor-on-their-device-thanks-to-the-baidu-sdk-495673.shtml>
17. *November 3, Softpedia* – (International) **Windows legacy layer used to bypass EMET security measures.** Security researchers from Duo Labs discovered that the Windows WoW64 subsystem used to support older or newer 32-bit applications on 64-bit architectures can be leveraged to bypass security measures added by Microsoft with the introduction of the Enhanced Mitigation Experience Toolkit (EMET) that was specifically designed to inspect 32-and 64-bit processes, allowing for more targeted attacks.
Source: <http://news.softpedia.com/news/windows-legacy-layer-used-to-bypass-emet->

[security-measures-495691.shtml](#)

18. *November 3, Softpedia* – (International) **Google researchers find 11 zero-day bugs in Samsung Galaxy S6 Edge.** Google's Project Zero security team identified 11 zero-day vulnerabilities in Samsung's Galaxy S6 Edge phone after the team began investigating new flaws when Samsung adapted the Android operating system (OS) to its custom hardware setup. Samsung fixed 8 of the vulnerabilities during its October Maintenance Release, and the other 3 vulnerabilities are scheduled to be resolved by November.
Source: <http://news.softpedia.com/news/google-researchers-find-11-zero-day-bugs-in-samsung-galaxy-s6-edge-495694.shtml>
19. *November 2, Securityweek* – (International) **Flaw in SAP firm's XSS filter exposed many sites to attacks.** A security researcher identified a reflective cross-site scripting (XSS) flaw on SuccessFactors, a SAP-owned company, and discovered that about 100 Web sites were exposed to the XSS filter, potentially allowing attackers to easily bypass Web pages due to the developers' failure to escape certain strings when sanitizing user input.
Source: <http://www.securityweek.com/flaw-sap-firms-xss-filter-exposed-many-sites-attacks>
20. *November 2, IDG News Service* – (International) **Google patches critical media processing flaws in Android.** Google released security patches for Nexus devices running both Android 5.1 (Lollipop) and 6.0 (Marshmallow) versions addressing seven vulnerabilities, two of which are critical and can be exploited remotely via specially crafted media files including sending multimedia messaging service (MMS) messages and deceiving users to play media in the browsers. The flaws are located in the mediaserver, libstagefright, Bluetooth, Telephony, and libutils components of Android.
Source: <http://www.computerworld.com/article/3000492/security/google-patches-critical-media-processing-flaws-in-android.html>

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

Communications Sector

See item [16](#)

Commercial Facilities Sector

21. *November 2, KTXL 40 Sacramento* – (California) **3 fires at same storage facility suspicious, investigators say.** Sacramento fire officials are investigating 3 fires that occurred over a 24-hour period at a Life Storage facility and damaged about 10 vehicles including RV's, trailers, boats, and cars November 1 – 2. No injuries were

reported and officials estimated the fire caused thousands of dollars in damage
Source: <http://fox40.com/2015/11/02/3-fires-at-same-storage-facility-suspicious-investigators-say/>

22. *November 1, WREG 3 Memphis; Associated Press* – (Missouri) **Man arrested in string of St. Louis black church fires.** Authorities arrested and charged a St. Louis man October 30 for 2 counts of second-degree arson after setting Ebenezer Lutheran Church and New Life Missionary Baptist Church ablaze following a string of church fires in the area between October 8 and October 22. Investigations into the other church fires are ongoing.

Source: <http://wreg.com/2015/11/01/man-arrested-in-string-of-st-louis-black-church-fires/>

Dams Sector

Nothing to report



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

- | | |
|-------------------------------------|---|
| Content and Suggestions: | Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590 |
| Subscribe to the Distribution List: | Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes . |
| Removal from Distribution List: | Send mail to support@govdelivery.com . |

Contact DHS

- To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
- To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.